Electronic Version
Stylesheet Version v1.1.1

Claims

[c1] What is claimed is:

1.An apparatus for calculating a TKIP Sbox value required by the TKIP Sbox function described in the IEEE P802.11i specification, the apparatus comprising:
a first plurality of combinatorial logic for calculating a TKIP Sbox left value according to a low part of an index value;
a second plurality of combinatorial logic for calculating a TKIP Sbox right value according to a high part of the index value; and
a third plurality of combinatorial logic for calculating the TKIP Sbox value according to the TKIP Sbox left value and the TKIP Sbox right value.

[c2] 2.The apparatus of claim 1, wherein the third plurality of combinatorial logic is a plurality of XOR gates.

[c3] 3.The apparatus of claim 2, wherein the TKIP Sbox left value is XORed with the TKIP Sbox right value by the plurality of XOR gates and the output of the plurality of XOR gates forms the TKIP Sbox value.

[c4] 4. The apparatus of claim 1, wherein for each bit in the

TKIP Sbox left value, the first plurality of combinatorial logic comprises a logic circuit, each logic circuit respectively calculating a bit in the TKIP Sbox left value.

[c5] 5.The apparatus of claim 1, wherein for each bit in the TKIP Sbox right value, the second plurality of combinatorial logic comprises a logic circuit, each logic circuit respectively calculating a bit in the TKIP Sbox right value.

[c6] 6.A method for calculating a TKIP Sbox value required by the TKIP Sbox function described in the IEEE P802.11i specification, the method comprising the following steps:
calculating a TKIP Sbox left value according to a first part of an index value;
calculating a TKIP Sbox right value according to a second part of the index value; and
calculating the TKIP Sbox value according to the TKIP Sbox left value and the TKIP Sbox right value.

[c7] 7.The method of claim 6, wherein the step of calculating the TKIP Sbox value comprises:
performing an exclusive-or of the TKIP Sbox left value and the TKP Sbox right value to form the TKIP Sbox value.

[c8] 8.The method of claim 6, wherein the step of calculating

the TKIP Sbox left value further comprising calculating each bit in the TKIP Sbox left value according to the first part of an index value.

[c9] 9.The method of claim 6, wherein the step of calculating the TKIP Sbox right value further comprising calculating each bit in the TKIP Sbox right value according to the second part of an index value.

[c10] 10.An apparatus for calculating a TKIP Sbox value required by a TKIP Sbox function, the apparatus comprising:

a TKIP Sbox logic configured to calculate a TKIP Sbox value according to an index value.

[c11] 11.The apparatus of claim 10, wherein the TKIP Sbox logic further comprises:

a first plurality of combinatorial logic for calculating a TKIP Sbox left value according to a first part of the index value;

a second plurality of combinatorial logic for calculating a TKIP Sbox right value according to a second part of the index value; and

a third plurality of combinatorial logic for calculating the TKIP Sbox value according to the TKIP Sbox left value and the TKIP Sbox right value.

[c12] 12.The apparatus of claim 11, wherein the third plurality of combinatorial logic is a plurality of XOR gates.

[c13] 13. The apparatus of claim 12, wherein the TKIP Sbox left value is XORed with the TKIP Sbox right value by the plurality of XOR gates and the output of the plurality of XOR gates forms the TKIP Sbox value.

[c14] 14.The apparatus of claim 11, wherein for each bit in the TKIP Sbox left value, the first plurality of combinatorial logic comprises a logic circuit, each logic circuit respectively calculating a bit in the TKIP Sbox left value.

[c15] 15.The apparatus of claim 11, wherein for each bit in the TKIP Sbox right value, the second plurality of combinatorial logic comprises a logic circuit, each logic circuit respectively calculating a bit in the TKIP Sbox right value.